

IEM®

Flow

Copyright

Copyright

Flow

Die Software Flow dient zur Konfiguration und Darstellung von Messungen mit dem Mobil-O-Graph[®] und dem HeartX Recorder.



IEM GmbH

Gewerbepark Brand 42
52078 Aachen
Deutschland

Email: info@iem.de

Internet: www.iem.de

Der Inhalt dieses Dokuments darf ohne schriftliche Genehmigung der IEM GmbH weder vervielfältigt noch veröffentlicht werden.

Die Software Flow ist urheberrechtlich geschützt und ist Eigentum des Herstellers. Es sind alle Rechte vorbehalten. Flow darf nicht ausgelesen, kopiert, dekompiert, zurückentwickelt, zerlegt oder in ein von Menschen lesbares Format gebracht werden. Alle Rechte der Nutzung und des Besitzes an der Software verbleiben bei der IEM GmbH.

© IEM GmbH 2026 Alle Rechte vorbehalten.

Inhaltsverzeichnis

1	Installation der Software.....	4
1.1	IT-Sicherheitsvorgaben.....	4
1.2	Systemvoraussetzungen.....	5
1.3	Software installieren.....	6
1.3.1	Benachrichtigungssymbol.....	7
2	Einstellungen.....	8
2.1	Speicherorte.....	8
2.2	Update.....	8
2.3	Kabelliste.....	8
2.4	Schnittstellen und Kommunikationswege.....	9
2.4.1	Einrichtung der Holter-Schnittstelle.....	11
2.4.2	GDT.....	11

1 Installation der Software

Neuinstallation

Stellen Sie vor der Installation von Flow sicher, dass alle Systemvoraussetzungen erfüllt sind, siehe [1.2 Systemvoraussetzungen, S. 5](#).

Laden Sie die aktuelle Version von Flow unter der folgenden URL herunter: www.iem.de/flow/download

Folgen Sie den Anweisungen in Kapitel [1.3 Software installieren, S. 6](#), um die Software zu installieren.

Online-Update-Service der vorhandenen Installation

Flow prüft diesen Dienst regelmäßig auf Aktualisierungen und bietet dem Benutzer an, bei Bedarf auf die neueste Version zu aktualisieren.

1.1 IT-Sicherheitsvorgaben

Die nachfolgend genannten Controls sind in die Risikobetrachtung bzgl. Cybersecurity eingeflossen und bilden die Grundlage für den sicheren Betrieb der Software und die Sicherheit der von der Software benötigten Daten. Eine nur teilweise Umsetzung der Controls führt zu einem erhöhten Sicherheitsrisiko bzgl. der Vertraulichkeit, Integrität und Verfügbarkeit.

Verschlüsseltes Dateisystem

- Verwendung eines Speicherorts, der starke Verschlüsselung unterstützt (z.B. LUKS, BitLocker, VeraCrypt).
- Sichere Verwaltung der Verschlüsselungsschlüssel.
- Der Zugriff auf unverschlüsselte Daten muss während des Betriebs ausschließlich autorisierten Prozessen vorbehalten sein.

Verschlüsselte Datenkommunikation

- Wenn auf die Daten über ein Netzwerk zugegriffen wird (z.B. Netzlaufwerk, Fernzugriff), muss die Kommunikation durch aktuelle kryptografische Protokolle gesichert werden (z.B. TLS 1.3, IPsec, SSH).
- Unverschlüsselte (Klartext-)Übertragungen (z.B. über FTP oder SMBv1) sind strikt untersagt.

Strikte Zugriffsbeschränkungen

- Zugriffsrechte müssen regelmäßig überprüft und dokumentiert werden.
- Zugriff darf nur Personen gewährt werden, die ein berechtigtes Need-to-know haben.

Backup-Strategie

Die Backup-Strategie verringert die Wahrscheinlichkeit eines Datenverlusts und ermöglicht es dem Betreiber, Ressourcen innerhalb des erwarteten Zeitrahmens wiederherzustellen. Die Backup-Strategie umfasst außerdem eine Sicherheitsrichtlinie (einschließlich moderner Datenverschlüsselung) sowie eine Zugriffsrichtlinie, um den Zugriff durch unbefugte Dritte zu verhindern.

Monitoring & Logging

Monitoring ermöglicht die frühzeitige Erkennung von Systemstörungen. Eine intelligente Logdateianalyse erlaubt es dem Betreiber zudem, Eindringlinge oder Schadsoftware zu erkennen.

Netzwerk und Firewall

Firewalls und Paketfilter verhindern schädlichen Netzwerkverkehr und -kommunikation. Intelligente Netzwerksegmentierung erhöht die Zuverlässigkeit und Verfügbarkeit, falls Ressourcen kompromittiert werden.

Schutz vor Schadsoftware/Malware-Schutz

Malware-Schutz auf Servern und Desktop-Rechnern erhöht die Sicherheit der Infrastruktur.

Strikte Zugriffskontrolle und sichere Passworrichtlinien

Strikte Zugriffskontrolle

- Prinzip der minimalen Rechtevergabe (Least Privilege)
- Multi-Faktor-Authentifizierung (MFA)
- Rollenbasierte Zugriffskontrolle
- Just-in-Time-Admin-/Break-Glass-Konten

Sichere Passworrichtlinie

- Mindestlängen
- Einsatz von Passwortmanagern
- Sperrmechanismen bei Fehlversuchen

Notfallplan

Ein Notfallplan nach Vorgabe des BSI (100-4: Notfallmanagement) erhöht die Wahrscheinlichkeit der Wiederherstellung der Systeminfrastruktur aufgrund eines sicherheitsbedingten Vorfalls.

DNS-Konfiguration

Die Applikation nutzt für die Namensauflösung des Online-Update Service die über das System bereitgestellten Einstellungen. Die korrekte Konfiguration der Einstellungen, sowie die Überprüfung der Authentizität des DNS Dienstes verringert die Wahrscheinlichkeit eines böartigen Angriffs.

Zur Sicherstellung der Integrität des Update-Pakets wurden weitere Sicherungsmaßnahmen implementiert.

Keine sicherheitskritischen Anwendungen auf dem Computer

Das Computersystem, auf dem die Anwendung betrieben wird, ist nicht für sicherheitsrelevante (Safety) oder unternehmenskritische Funktionen vorgesehen.

SBoM

Die SBoM (Software Bill of Materials) liegt im Installationsverzeichnis im Unterordner **SBOM**. Die SBoM liegt als CycloneDX-Dokument im Json-Format vor. Es wird empfohlen, die darin enthaltenen Fremdbibliotheken in das interne Überwachungssystem aufzunehmen.

1.2 Systemvoraussetzungen

Unterstützte, medizinische Geräte

- Mobil-O-Graph[®] mit Firmware 200007 (GTIN: 04041346100104, 04041346102111) mit 4-Pin Kabel (GTIN: 04041346101934)
- Mobil-O-Graph[®] mit Firmware 200212 (GTIN: 04041346100784, 04041346102269) mit 4-Pin Kabel (GTIN: 04041346101934)
- HeartX Recorder (GTIN: 04250903203176), für KI-Service

Installation der Software

- HeartX Recorder (GTIN: 04250903203398)

Betriebssystem

Bitte beachten Sie: Für die Installation der Software werden Administratorrechte benötigt.

Microsoft	Windows® 10, Windows® 11
Apple	macOS® 26 (Tahoe)

Minimale Systemanforderungen

Bildschirmgröße (Diagonale)	14 Zoll
Bildschirmauflösung (in Pixel)	1280 x 720
Festplattenspeicher (in GB)	1 GB ständig freier Speicherplatz (wird für die Log-Dateien der Software benötigt)
Schnittstelle für Geräteanschluss	USB Typ A (zum Anschluss des Mobil-O-Graph®)
Optional	Netzwerkadapter mit Internetzugang: <ul style="list-style-type: none">• Für zukünftige Aktualisierungen der Software über den integrierten Online-Update-Service

Betriebssystem abhängige Systemanforderungen

	Microsoft Windows® 10, 11	macOS® 15, Sequoia
Arbeitsspeicher (RAM), Minimum	4 GB	8 GB
Prozessor	x86 Intel Core i5 oder entsprechendes AMD-Pendant	x86 Intel Core i5 Apple Silicon

1.3 Software installieren

Vorbereitungen

- Stellen Sie sicher, dass die Systemvoraussetzungen erfüllt sind, siehe 1.2 Systemvoraussetzungen, S. 5
- Laden Sie die aktuelle Version von Flow unter der folgenden URL herunter: www.iem.de/flow/download

Durchführung


1. Starten Sie die Installationsdatei für Ihr Betriebssystem:

Microsoft Windows®	macOS®
flow-<version>-windows-amd64.exe	flow-<version>-macos-amd64.dmg (x86 Intel Prozessor)
	flow-<version>-macos-aarch64.dmg (Apple Silicon Prozessor)

2. Folgen Sie den Anweisungen des **Flow-Einrichtungsassistenten**. Am Ende der Installation haben Sie die Möglichkeit, Autostart für Flow einzustellen.

- Ist die Software bereits auf dem Computer installiert und Sie starten die Installation erneut, erkennt der **Flow-Einrichtungsassistent** automatisch die bereits vorhandene Installation samt Installationsverzeichnis. Bei einer erneuten Installation bleiben alle Daten und bereits vorgenommenen Einstellungen erhalten.

1.3.1 Benachrichtigungssymbol

Wenn Sie die Software erfolgreich installiert und gestartet haben, finden Sie das Benachrichtigungssymbol 

- unter Windows[®] im rechten, unteren Teil der Taskleiste. Sehen Sie das Symbol nicht, müssen Sie vielleicht das Menü mittels Pfeil aufklappen, um alle aktiven Anwendungen sehen zu können.
- unter macOS[®] im rechten, oberen Teil der Menüleiste.

Beenden der Software im Benachrichtigungssymbol

Windows[®]:

Klicken Sie mit der sekundären Taste auf das Symbol der Software, um die Software zu beenden.

macOS[®]:

Klicken Sie mit der primären Taste auf das Symbol der Software, um die Software zu beenden.

2 Einstellungen



Sie erreichen das Menu für Einstellungen über das Zahnrad links oben in der Benutzeroberfläche.

2.1 Speicherorte

Speicherort für Berichte

Sie wählen den Speicherort, in dem die Software alle Berichte ablegt. Diese Einstellung muss beim ersten Start der Software definiert werden und kann später verändert werden. Bitte stellen Sie sicher, dass die Software für den gewählten Ordner Lese- und Schreibrechte hat.

Achtung

Multi room

Die Funktion "Multi room" ermöglicht es, dass mehrere Software-Instanzen auf dieselben Jobdaten zugreifen können.

Wählen Sie einen Speicherort, für den alle Software-Instanzen Lese- und Schreibrechte haben.

Bitte beachten Sie, dass je nach Netzwerkkonfiguration Zeitverzögerungen für den Zugriff auf den gemeinsamen Speicherort entstehen können, so dass Änderungen an Jobs verzögert in allen verbundenen Software-Instanzen sichtbar werden.

2.2 Update

Voraussetzung für die Nutzung des Online-Update-Services ist eine Internetverbindung sowie Administratorrechte für die Installation.

Die Software besitzt einen integrierten Online-Update-Service. FLOW überprüft diesen Dienst regelmäßig, ob eine neue Programmversion verfügbar ist. Sobald ein Update verfügbar ist, lädt die Software das Programm herunter und informiert den Benutzer, dass eine neue Version installiert werden kann. Der Benutzer kann das Update jederzeit starten.

Während des Updates schließt sich die Software und startet automatisch nach Abschluss des Updates.

Daten und Einstellungen werden während des Updates auf die neue Programmversion übertragen.

Achtung

Sicherheitskritische Updates

Kritische Updates beheben sicherheitsrelevante Probleme. Sie müssen installiert werden, damit FLOW weiterhin funktioniert.

2.3 Kabelliste

Die Software fordert die Benutzer auf, alle verwendeten 4-Pin Kabel für diese Software zu registrieren bzw. festzulegen, dass sie nicht für diese Software genutzt werden.

Damit werden unerwünschte Wechselwirkungen mit anderen Geräten und Kabeln, die an den Computer angeschlossen werden, verhindert.

Die Funktion "Kabelliste" ermöglicht, alle gespeicherten Informationen zu 4-Pin Kabeln zu löschen. Diese Funktion sollte genutzt werden, wenn ein 4-Pin Kabel falsch kategorisiert wurde.

2.4 Schnittstellen und Kommunikationswege

Allgemein

Applikationsupdates / Microsoft Azure	
Ziel-ID	A2916
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443
Endpunkt / Beschreibung	cd.iem.zone/flow
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	Internetverbindung mit Port 443 erforderlich

IEM Sentry Service	
Ziel-ID	A4941
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443
Endpunkt / Beschreibung	o4510141214621696.ingest.de.sentry.io/
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	Internetverbindung mit Port 443 erforderlich

IEM Website FLOW Anwendung, Release Notes, Geräte-Firmware, Datenschutzbestimmungen	
Ziel-ID	A3589
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443
Endpunkt / Beschreibung	iem.de
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	Internetverbindung mit Port 443 erforderlich

ABDM

IEM Mobil-O-Graph	
Ziel-ID	A2926
Richtung	Lokales I/O
Protokoll / Port	USB/ UART
Endpunkt / Beschreibung	Externes Aufnahmegerät

Einstellungen

IEM Mobil-O-Graph	
Sicherheitsmaßnahmen	-
Hinweise für Betreiber	Sicherer physischer USB-Anschluss

Holter

IEM HeartX Holter	
Ziel-ID	A4585
Richtung	Lokales I/O
Protokoll / Port	USB
Endpunkt / Beschreibung	Externes Aufnahmegerät
Sicherheitsmaßnahmen	-
Hinweise für Betreiber	Sicherer physischer USB-Anschluss

Azure-Speicher / Hochladen von Holter-Messungen.	
Ziel-ID	A5078
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443
Endpunkt / Beschreibung	gtmhxhcustomers05.blob.core.windows.net
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	Internetverbindung mit Port 443 erforderlich

ECG AI backend	
Ziel-ID	A4588
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443
Endpunkt / Beschreibung	hxh-api.prod.heartxholter.com
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	Internetverbindung mit Port 443 erforderlich

Webviewer	
Ziel-ID	A5072
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443

Webviewer	
Endpunkt / Beschreibung	heartxholter.com
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	Internetverbindung mit Port 443 erforderlich

2.4.1 Einrichtung der Holter-Schnittstelle

Voraussetzung: HeartX Recorder (GTIN: 04250903203176) und Account für [Webviewer](#)

Um die Schnittstelle zum KI-Auswerteservice für den HeartX Recorder einzurichten, gehen Sie wie folgt vor:

- Melden Sie sich mit Ihrem Account im [Webviewer](#) an
- Öffnen Sie die Einstellungen (Zahnrad)
- Klicken Sie auf den Eintrag "IEM Integration"
- Erstellen Sie ein Token mit einem Klick auf **Create Token**. Es wird automatisch eine .token Datei heruntergeladen.
- Hinterlegen Sie die Datei in den Einstellungen zum HeartX. Die Dateibenennung muss unverändert bleiben!

2.4.2 GDT

FLOW bietet Betreibern die Möglichkeit, eine Datenschnittstelle zu einem Praxisverwaltungssystem (PVS) oder Krankenhausinformationssystem (KIS) unter Verwendung des GDT 2.1-Standards (Gerätedatentransfer) zu konfigurieren.

Damit FLOW einen Job aus dem gewünschten System annehmen und verwerten kann, sind die Informationen folgender Codes in der Datei erforderlich, die an FLOW gesendet wird:

- 3000 - Patientenkenung
- 8000 - erwarteter Wert "6302"
- 8402 - erwarteter Wert:
 - für ABDM "BDM01"
 - für Holter "EKG04"

Die GDT-Spezifikation definiert nur die Dateistruktur und Semantik, enthält jedoch keine Sicherheitsmechanismen wie Verschlüsselung, Authentifizierung oder Integritätsschutz. Der Datenaustausch erfolgt über gemeinsam genutzte Verzeichnisse („GDT-Austauschordner“). Der Betrieb und Schutz dieser Verzeichnisse liegt in der Verantwortung des Betreibers (z. B. der Arztpraxis oder des IT-Dienstleisters). Die Anwendung unterstützt den Datenaustausch streng innerhalb der GDT-Spezifikation. End-to-End-Sicherheitsmechanismen (wie Verschlüsselung oder digitale Signaturen) sind nicht Teil des Standards und daher nicht implementiert.

Um einen sicheren und konformen Betrieb zu gewährleisten, muss der Betreiber folgende Maßnahmen ergreifen:

- Zugangskontrollmaßnahmen implementieren. Nur autorisierte Stellen dürfen auf die HIS-GDT-Schnittstelle zugreifen.
- Die Integrität und Vertraulichkeit der GDT-Dateiübertragungen sicherstellen.

Einstellungen

- Speicherte Informationen durch Verschlüsselung und technische Sicherheitsvorkehrungen schützen.
- Die Protokollierung und Überwachung des GDT-Austauschs zur Rechenschaftspflicht aufrechterhalten.
- Angemessene Sicherungs- und Wiederherstellungsmechanismen bereitstellen, um die Verfügbarkeit der ausgetauschten GDT-Dateien zu gewährleisten.

Achtung

Multi room

Die Funktion "Multi room" ermöglicht es, dass mehrere Software-Instanzen auf dieselben Jobdaten zugreifen können.

Stellen Sie dafür sicher, dass in allen Instanzen, die über Multi room verbunden werden sollen, folgende Einstellungen übereinstimmen:

- GDT Modus eingeschaltet
 - Zeichensatz Encoding
 - Import- und Exportverzeichnisse
Es müssen die gleichen Verzeichnisse eingestellt sein, die für den jeweiligen Arbeitsplatz auch als Austauschordner für das PVS/KIS konfiguriert wurden.
-